- 10-

CLAIMS

WHAT IS CLAIMED IS:

1. A system for locking/unlocking a mobile banking function, the system comprising:

a mobile communication terminal (10), which includes an embedded or external IC card chip(11) in which personal financial information for supporting a banking function is stored, when the mobile communication terminal (10) receives a chip blocking SMS message for maintaining the personal financial information stored in the IC card chip (11) in a locking state, the mobile communication terminal (10) restricting access to the IC card chip (11) by driving an internal chip driver (12), and when the mobile communication terminal (10) receives a chip blocking unlocking SMS message for unlocking the locking state of the personal financial information, the mobile communication terminal (10) permitting access to the IC card chip (11) by driving the chip driver (12);

a common carrier banking server (40), which communicates with the mobile communication terminal (10) via a wireless base station (20) and a short message service center (SMSC) (30) and transmits a chip blocking SMS message or a chip blocking unlocking SMS message to the mobile communication terminal (10) when receiving a chip blocking or chip blocking unlocking request from a financial organ issuing the IC card chip; and

a financial organ host (50), which transmits a chip blocking request to the common carrier banking server (40) when receiving a theft and loss report from a user of the mobile communication terminal (10), and which transmits a chip blocking unlocking request to the common carrier banking server (40) when receiving a request for the reuse of the mobile

- 11 -

communication terminal (10) for which a theft and loss report has been filed from the user.

2.   The system according to Claim 1, wherein the chip driver (12) embedded in the mobile communication terminal (10) restricts or permits access to the IC card chip (11) of the mobile communication terminal (10) when the mobile communication terminal (10) requests chip blocking or chip blocking unlocking after receiving a chip blocking SMS message or a chip blocking unlocking SMS message.

3.   The system according to Claim 1, wherein the common carrier banking server (40) transmits the contents of receipt to the financial organ host (50) when receiving a theft and loss report of the mobile communication terminal (10) from a user of the mobile communication terminal (10) or receiving a request for the reuse of the mobile communication terminal (10) for which the theft and loss report has been filed from the user.

4.   The system according to Claim 1, wherein the financial organ host (50) transmits a chip blocking request to the common carrier banking server (40) when receiving the theft and loss report of the user of the mobile communication terminal (10) from the common carrier banking server (40) and transmits a chip blocking unlocking request to the common carrier banking server (40) when receiving a request of the reuse of the mobile communication terminal (10) for which the theft and loss report has been filed from the common carrier banking server (40).

5.   A method of locking/unlocking a mobile banking function, the method comprising:

- 12-

(S10) when receiving a theft and loss report of a mobile communication terminal (10) from a user of the mobile communication terminal (10) or receiving a request for the reuse of the mobile communication terminal (10) for which the theft and loss report has been filed from the user, requesting chip blocking or chip blocking unlocking of a common
5   carrier banking server (40);

(S20) transmitting a chip blocking short message service (SMS) message or a chip blocking unlocking SMS message to the corresponding mobile communication terminal (10) via a wireless base station (20) and a PSDN (30);

(S30) determining whether or not the SMS message received from the common
10   carrier banking server (40) is the chip blocking SMS message or the chip blocking unlocking SMS message;

(S40) if it is determined that the SMS message received by the mobile communication terminal (10) is the chip blocking SMS message, driving an internal chip driver (12) of the mobile communication terminal (10) to restrict access to an embedded or
15   external IC card chip (11) of the mobile communication terminal (10) so that personal financial information stored in the IC card chip (11) is maintained in a locking state; and

(S50) if it is determined that the SMS message received by the mobile communication terminal (10) is the chip blocking unlocking SMS message, driving the internal chip driver (12) of the mobile communication terminal (10) to permit access to the
20   embedded or external IC card chip (11) of the mobile communication terminal (10) so that the personal financial information stored in the IC card chip (11) is unlocked.